

AD-A264 271



2

NAVAL WAR COLLEGE

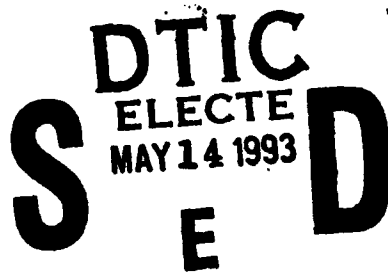
Newport, R.I.

CREATING THE COMMAND AND CONTROL DIFFERENTIAL

by

JANE A. BOYD

MAJ, USA



A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Operations.

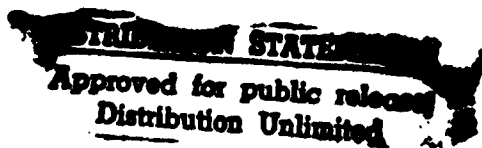
The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: \_\_\_\_\_

*Jane A. Boyd*

93 5 11 25 8

18 June 1993



93-10406



# REPORT DOCUMENTATION PAGE

<b>1a REPORT SECURITY CLASSIFICATION</b> UNCLASSIFIED			<b>1b RESTRICTIVE MARKINGS</b>														
<b>2a SECURITY CLASSIFICATION AUTHORITY</b>			<b>3 DISTRIBUTION/AVAILABILITY OF REPORT</b> DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE, DISTRIBUTION IS UNLIMITED														
<b>2b DECLASSIFICATION/DOWNGRADING SCHEDULE</b>			<b>5 MONITORING ORGANIZATION REPORT NUMBER(S)</b>														
<b>4 PERFORMING ORGANIZATION REPORT NUMBER(S)</b>			<b>7a NAME OF MONITORING ORGANIZATION</b>														
<b>6a NAME OF PERFORMING ORGANIZATION</b> OPERATIONS DEPARTMENT		<b>6b OFFICE SYMBOL</b> (If applicable) C	<b>7b ADDRESS (City, State, and ZIP Code)</b>														
<b>6c ADDRESS (City, State, and ZIP Code)</b> NAVAL WAR COLLEGE NEWPORT, R.I. 02841		<b>9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER</b>															
<b>8a NAME OF FUNDING/SPONSORING ORGANIZATION</b>		<b>8b OFFICE SYMBOL</b> (If applicable)	<b>10 SOURCE OF FUNDING NUMBERS</b>														
<b>8c ADDRESS (City, State, and ZIP Code)</b>		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%;">PROGRAM ELEMENT NO.</td> <td style="width: 25%;">PROJECT NO.</td> <td style="width: 25%;">TASK NO.</td> <td style="width: 25%;">WORK UNIT ACCESSION NO.</td> </tr> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </table>				PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT ACCESSION NO.								
PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT ACCESSION NO.														
<b>11 TITLE (Include Security Classification)</b> CREATING THE COMMAND AND CONTROL DIFFERENTIAL (U)																	
<b>12 PERSONAL AUTHOR(S)</b> MAJ JANE A. BOYD, USA																	
<b>9. TYPE OF REPORT</b> FINAL		<b>13b TIME COVERED</b> FROM                      TO		<b>14 DATE OF REPORT (Year, Month, Day)</b> 2/22/93													
<b>15 PAGE COUNT</b> 40		<b>16 SUPPLEMENTARY NOTATION</b> A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Operations. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.															
<b>17 COSATI CODES</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 33%;">FIELD</th> <th style="width: 33%;">GROUP</th> <th style="width: 33%;">SUB-GROUP</th> </tr> <tr> <td> </td> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> </tr> </table>			FIELD	GROUP	SUB-GROUP										<b>18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)</b> COMMAND AND CONTROL, COMMAND, CONTROL AND COMMUNICATIONS, COMMAND, CONTROL, COMMUNICATIONS COUNTERMEASURES		
FIELD	GROUP	SUB-GROUP															
<b>19 ABSTRACT (Continue on reverse if necessary and identify by block number)</b> THIS PAPER PROPOSES THAT JOINT PLANNING AND EMPLOYMENT OF COMMAND, CONTROL AND COMMUNICATIONS COUNTERMEASURES (C3CM) IS KEY TO ENSURING THE COMMAND AND CONTROL (C2) DIFFERENTIAL. THE C2 PROCESS AND THE INTELLIGENCE CYCLE INTERACTION IS EXAMINED ALONG WITH THE C2 DIFFERENTIAL. THE COMPLEX C3CM MISSIONS ARE EXPLAINED INCLUDING HOW THE USE OF C3CM TOOLS CAN IMPACT THE C2 PROCESS. RECOMMENDATIONS FOR IMPROVED UTILIZATION OF C3CM ARE PROPOSED, TO INCLUDE: DEDICATED TEAM OF EXPERTS ON THE JOINT STAFF, INCREASE C3 PROTECTION MISSIONS AND ENSURING C3 SYSTEMS INTEROPERABILITY.																	
<b>20 DISTRIBUTION/AVAILABILITY OF ABSTRACT</b> <input checked="" type="checkbox"/> UNCLASSIFIED/UNLIMITED <input type="checkbox"/> SAME AS RPT <input type="checkbox"/> DTIC USERS			<b>21 ABSTRACT SECURITY CLASSIFICATION</b> UNCLASSIFIED														
<b>22a NAME OF RESPONSIBLE INDIVIDUAL</b> CHAIRMAN, OPERATIONS DEPARTMENT			<b>22b TELEPHONE (Include Area Code)</b> 841-3414		<b>22c OFFICE SYMBOL</b> C												

DD FORM 1473, 84 MAR

 83 APR edition may be used until exhausted  
 All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

© U.S. Government Printing Office 1989-433-012

0102-LF-014-6602

CREATING THE COMMAND AND CONTROL DIFFERENTIAL

The Desert Storm experience and the explosion in electronic technologies have highlighted the need for a joint war fighting strategy that attacks the enemy's command and control process while protecting our own capabilities. Understanding the Command and Control (C<sup>2</sup>) process and the intelligence cycle interaction is key to the implementation of a joint strategy. By attacking key functions in enemy C<sup>2</sup> process, Command, Control, and Communications Countermeasures (C<sup>2</sup>CM) strategies can create the environment that enables friendly forces to act faster than enemy forces (the command and control differential). Successful execution of joint C<sup>2</sup>CM involves employment of joint assets in a integrated, synchronized, and coordinated manner. Although there are many considerations in employing joint C<sup>2</sup>CM strategies the following are key. First, the joint force commander should ensure a dedicated team of experts are on the joint staff to plan and conduct joint C<sup>2</sup>CM strategies. Component commands should mirror the emphasis by the joint commander. Second, C<sup>2</sup> protection, including operations security, must be emphasized to ensure that our command and control functions effectively and Counter C<sup>2</sup> measures are guarded. Last, critical intelligence and communications system problems, such as interoperability, need to be corrected for the command and control differential to be achieved.

## PREFACE

Throughout this paper the terms Command and Control (C2) systems and Command, Control and Communications (C3) systems are used. In recent publications the term Command, Control, Communications and Computer systems (C4) systems has replaced C2 systems, C3 systems, communications, and communications-electronics. To avoid confusion when discussing C3 countermeasures the term C3 systems is used to encompass all other terms associated with C3 and includes computer hardware and software.

Accession For	
NTIS CRA&I	<input checked="checked" type="checkbox"/>
DTIC TAB	<input checked="checked" type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification .....	
By .....	
Distribution /	
Availability Codes	
Dist	Avail and/or Special
A-1	

DTIC QUALITY INSPECTED 8

## TABLE OF CONTENTS

CHAPTER	PAGE
ABSTRACT.....	ii
PREFACE.....	iii
LIST OF ILLUSTRATIONS.....	v
I INTRODUCTION.....	1
The Problem.....	1
Thesis.....	1
Recommendations.....	2
II UNDERSTANDING THE DIFFERENTIAL.....	4
The Command and Control Process.....	4
Intelligence and the C <sup>2</sup> Process.....	5
The Command and Control Differential.....	10
III THE WAR FIGHTING STRATEGY.....	13
Counter C <sup>2</sup> .....	14
C <sup>2</sup> Protection.....	18
Intelligence and C <sup>2</sup> CM.....	19
Conclusions.....	22
IV IMPLEMENTING C <sup>2</sup> CM.....	23
C <sup>2</sup> CM in the Joint Environment: Integrated, Synchronized, Coordinated.....	23
Guarding the Indicators.....	24
Fixing Intelligence Cycle and C <sup>2</sup> Capabilities.....	25
V CONCLUSION.....	27
NOTES.....	29
BIBLIOGRAPHY.....	33

## LIST OF ILLUSTRATIONS

FIGURE		PAGE
1.	The Command and Control Process.....	6
2.	The Intelligence Cycle and the C <sup>2</sup> Process.....	9
3.	The Command and Control Differential.....	11
4.	C <sup>3</sup> CM Strategy.....	15
5.	C <sup>3</sup> CM, Intelligence and C <sup>2</sup> Process.....	21

# CREATING THE COMMAND AND CONTROL DIFFERENTIAL

## CHAPTER 1

### INTRODUCTION

**The Problem.** Desert Storm emphasized the critical role of Command, Control and Communications (C<sup>3</sup>) systems. For allied forces C<sup>3</sup> was not just a force multiplier but a force enabler. In addition, some of the first bombing targets were Saddam Hussein's command and control structure.<sup>1</sup> During this war, though, we faced an enemy that underestimated coalition abilities and allowed allied forces months to install sophisticated C<sup>3</sup> systems and make them interoperable.<sup>2</sup> As our adversaries also learn lessons from Desert Storm, U.S. forces may no longer have the advantages it had when fighting against the Iraqis. To create the command and control (C<sup>2</sup>) differential coalition forces enjoyed during Desert Storm, joint commanders need to use an integrated C<sup>3</sup>CM strategy based on knowledge of the C<sup>2</sup> process and intelligence cycle. This strategy may be the key to successful operations in the future.

**Thesis.** Joint Publication 1 calls for concentration of overwhelming joint forces, based on skillfulness of employment, seizing the initiative by taking calculated risks to throw the enemy off balance, and agility, which aims to out do the enemy's ability to think, plan, communicate and act.<sup>3</sup> The successful implementation of these principles of joint warfare are directly

related to the efficiency of the Joint Force Commander's (JFC) C<sup>2</sup> process in conjunction with an ineffective enemy C<sup>2</sup> process. If the JFC can create a positive differential between how fast friendly forces can act versus the enemy a ability to act the principles of joint warfare can be implemented.

The new doctrinal statement of joint operational concepts calls for the JFC to exploit the "information differential". This may be the key to "avoiding unnecessary and expensive operations, in terms of lives and national resources".<sup>4</sup> Today, the U.S. military enjoys superior intelligence and communications capabilities. We can assume an information differential with any potential adversary. This may not occur in the future as third world countries gain more space capabilities, anti-satellite weapons increase, high quality intelligence becomes increasingly available on the commercial market, and our own capabilities are degraded through defense cutbacks. In the future it will be increasingly necessary to use joint C<sup>2</sup>CM assets to create an information differential to gain an advantage in the C<sup>2</sup> process.

Recommendations. The JFC must be prepared to employ a combination of air, land, sea, special operations, and space capabilities as C<sup>2</sup>CM to blind the enemy and sever command links.<sup>5</sup> The JFC and dedicated team of experts must fully implement a joint war fighting concept based on C<sup>2</sup>CM to create the information and, correspondingly, the C<sup>2</sup> differential. This cannot be a piecemeal, fragmented effort delegated for the components to implement independently but one that incorporates all assets into a



synergistic war fighting strategy. The team must employ C<sup>2</sup>CM strategies that use the components tools of operations security, jamming, deception and selected destruction to perform the most effective Counter C<sup>2</sup> and critical C<sup>2</sup> Protection missions.

The JFC and the expert team needs to direct efforts towards C<sup>2</sup> Protection. First, C<sup>2</sup> Protection measures can and should be enforced through heightened training and awareness to increase our capability in wartime to create the C<sup>2</sup> differential. Operations Security (OPSEC) must be practiced in day-to-day actions to be effective during a crisis. Secondly, interoperable communications and reliable intelligence dissemination must be an enforced standard, not something that takes six months of reengineering efforts to accomplish. An ineffective C<sup>2</sup> process is created when forces lose the capability to communicate with each other and the feedback on events during the crisis. Until the communications and intelligence system problems are solved C<sup>2</sup>CM war fighting strategies can neither be fully effective or implemented.

In order to provide a baseline understanding of the joint use of C<sup>2</sup>CM strategies, the next chapter explains the C<sup>2</sup> process and its interaction with the intelligence cycle. Chapter III explains C<sup>2</sup>CM and how it can be used to create the C<sup>2</sup> differential. Chapter IV provides recommendations for the joint commander which, if implemented, will lead to successful C<sup>2</sup>CM war fighting strategies. The last chapter revisits the key issues on C<sup>2</sup>CM and the requirements for implementing an effective joint strategy.

## CHAPTER 11

### UNDERSTANDING THE DIFFERENTIAL

The Command and Control Process. Understanding the process that commanders, both friendly and enemy, use to control forces in the field is crucial to implementing strategies aimed at this critical center of gravity.

Command and Control (C<sup>2</sup>) has two purposes. It provides control over friendly forces while also acting to guide opponent decisions by occupying the enemy so completely that he can only respond and not initiate any actions. These purposes act in support of the accomplishment of the mission.<sup>1</sup>

C<sup>2</sup> can not be discussed without defining an important ingredient to its effectiveness. C<sup>2</sup> consists of a process followed to control forces and a system used to physically implement the process. This system, defined as Command, Control, Communications (C<sup>3</sup>), is the particular arrangement of personnel, equipment, communications, facilities, and procedures used by a commander to support decision making and control forces. C<sup>3</sup> is the central system that ties together the C<sup>2</sup> process. Effective employment and control of C<sup>3</sup> system resources to support the C<sup>2</sup> process are the responsibility of the joint commander.<sup>2</sup> Although the remainder of the discussion of C<sup>2</sup> will center on the process, the system is key to the efficiency of the process.

It is important to understand the steps of the C<sup>2</sup> process for

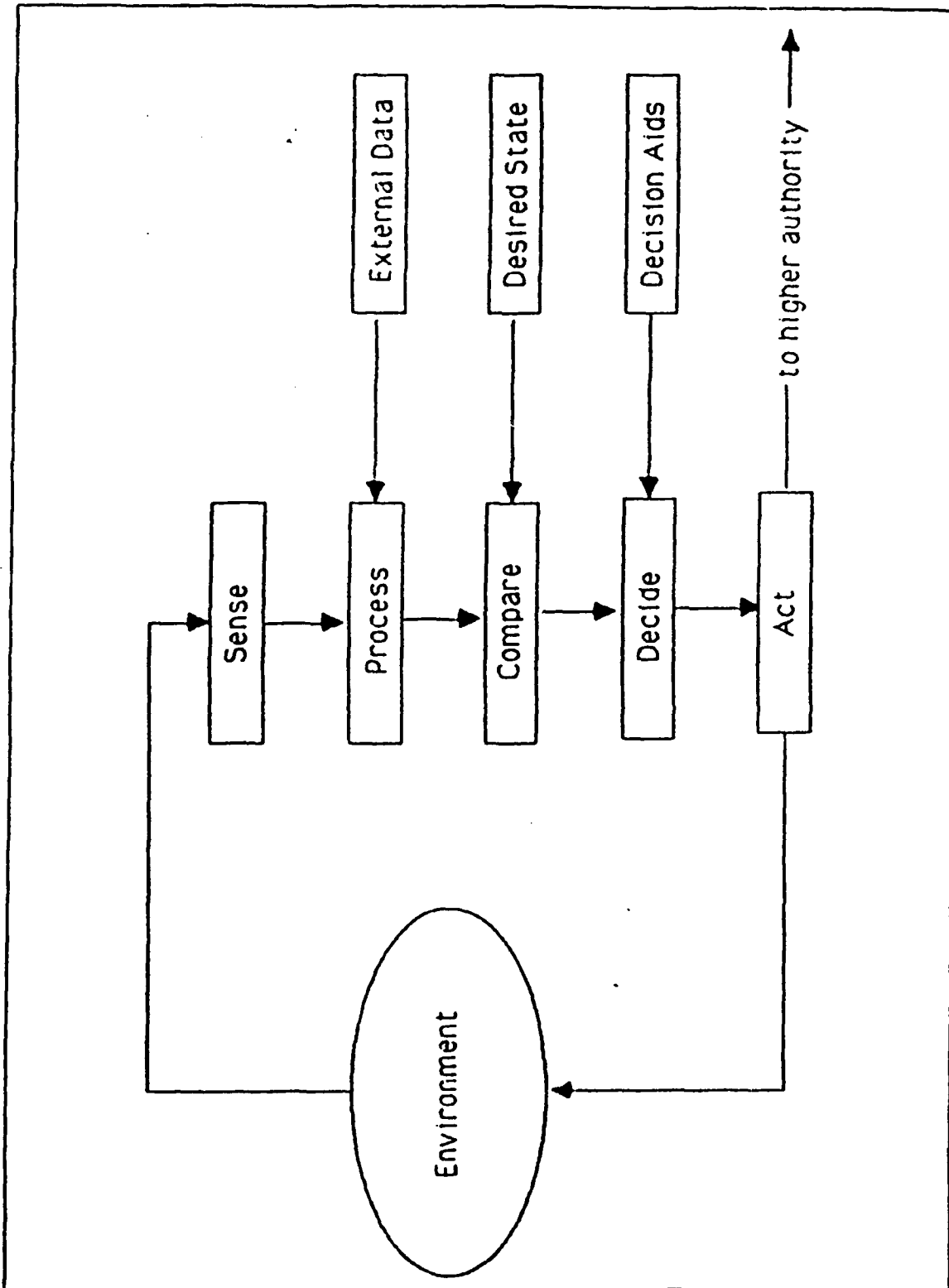
with this understanding strategies can be developed to guard friendly commanders most critical steps while disrupting the enemy's process.

Numerous models attempt to describe the C<sup>2</sup> process. One noted model, shown in Figure 1, was developed by Dr. Joel Lawson. There are five basic functions depicted in the model: SENSE, PROCESS, COMPARE, DECIDE, and ACT.<sup>2</sup>

The SENSE function involves all the data gathering activities, systems and procedures. It uses national and tactical assets to give the commander continuous and timely coverage of events and areas. The PROCESS function takes the raw data collected in the SENSE function and turns it into meaningful information. In the PROCESS function, fusion of intelligence data is performed. This fusion converts raw data from multiple sources into finished intelligence information for use in other functions. In the COMPARE function, the state of the environment determined from the information delivered by the PROCESS function is compared with a desired state. The DECIDE function determines the specific action that needs to be accomplished in order to change the current state of the environment to the desired state. Finally, the ACT function is the interface between the commander and the environment. It is the means by which decisions are directed and subordinate forces controlled. "

Intelligence and the C<sup>2</sup> Process. Intelligence is imperative for a commander to make decisions. It provides the SENSE function with the data necessary to begin the C<sup>2</sup> process. Without

FIGURE 1  
COMMAND AND CONTROL PROCESS



intelligence on enemy capabilities and assets, effective plans can not be developed nor can good decisions be made. Intelligence can provide the edge that comes from not only knowing what the enemy is doing, but also from anticipating what he will do next. The following sections explain the intelligence cycle, and show the interaction of intelligence in the C<sup>2</sup> process.

Intelligence is the product that results from evaluating, analyzing, integrating and interpreting all available information on one or more aspects of foreign nations or areas of operations.<sup>2</sup> Converting information into intelligence is a five step cycle.

Planning and direction involves determining the exact intelligence requirements and preparing a collection plan. The joint commander and staff provide needs for collection by identifying essential elements of information (EEIs). Once an intelligence requirements have been validated, orders and requests for information are issued to information collection assets. This process is dynamic and continuous checks are performed on the collection assets. Plans and directions are modified based on how well the intelligence produced actually satisfies user requirements.

Collection is the acquisition and delivery of information to the proper processing unit for producing intelligence. The full spectrum of collection systems have the capability to deliver vast quantities of detailed information but directed collection, based on EEIs, depends on how cooperative the enemy is and the type of collection efforts that are employed.

Processing is the conversion of information into a form that a

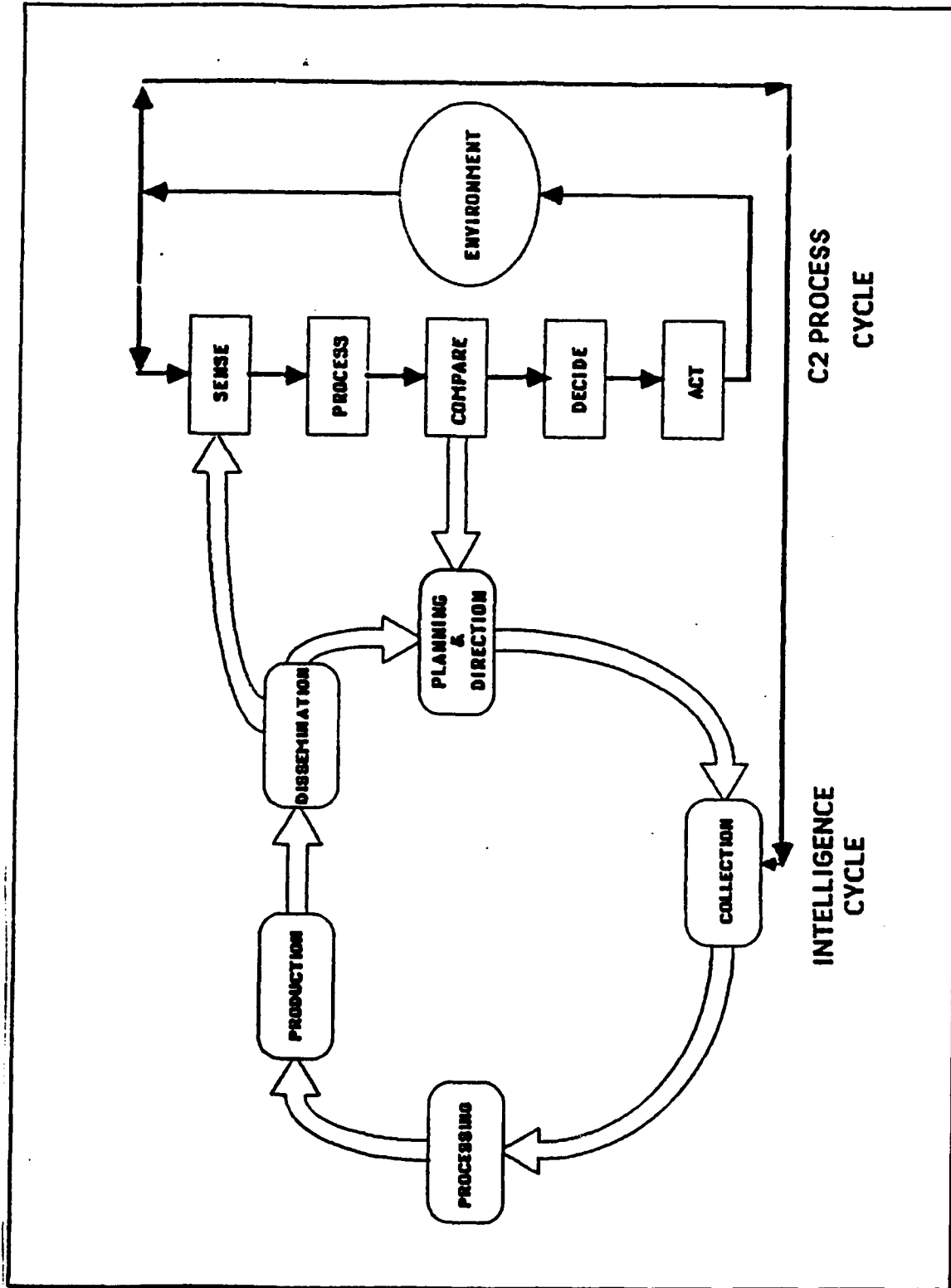
person or machine can use. Processing includes translation of foreign documents into the language of the user, converting photographic information in a form that can be inserted into a computer, or reformatting intelligence into compatible transmission standards. In the production stage, information is converted into finished intelligence through integration, analysis, evaluation and interpretation of all source data to support known or anticipated user requirements. This is where information from various sources is fused to give a complete picture, situation or event. At the CINC level this is accomplished at the Joint Intelligence Center (JIC).

Dissemination involves getting the intelligence to the user in a form he can understand. Without the delivery of intelligence to the user, the rest of the cycle is useless.<sup>4</sup>

This intelligence cycle is important for the C<sup>2</sup> to operate effectively. Figure 2 shows the interaction between the Intelligence cycle and the C<sup>2</sup> process. Intelligence helps the decision maker plan, structure, and employ forces to counter the enemy. The intelligence cycle interacts with and operates as a function to the C<sup>2</sup> process. The essential tasks of intelligence for the process are to assess and forecast changes in the enemy situation. These forecasts guide the C<sup>2</sup> SENSE functions by indicating where and when to look for more data and allow the DECIDE function to determine the best means to accomplish a given mission. The DECIDE function correlates available intelligence from the intelligence cycle with real time information. This intelligence aids the PROCESS function by providing a base to

FIGURE 2

THE INTELLIGENCE CYCLE AND C<sup>2</sup> PROCESS INTERACTION



identify the patterns that may signify important enemy activities. Because of the interrelationship of the intelligence and C<sup>2</sup> cycles, the timeliness and effectiveness of C<sup>2</sup> is dependent on the timeliness and effectiveness of the intelligence cycle.

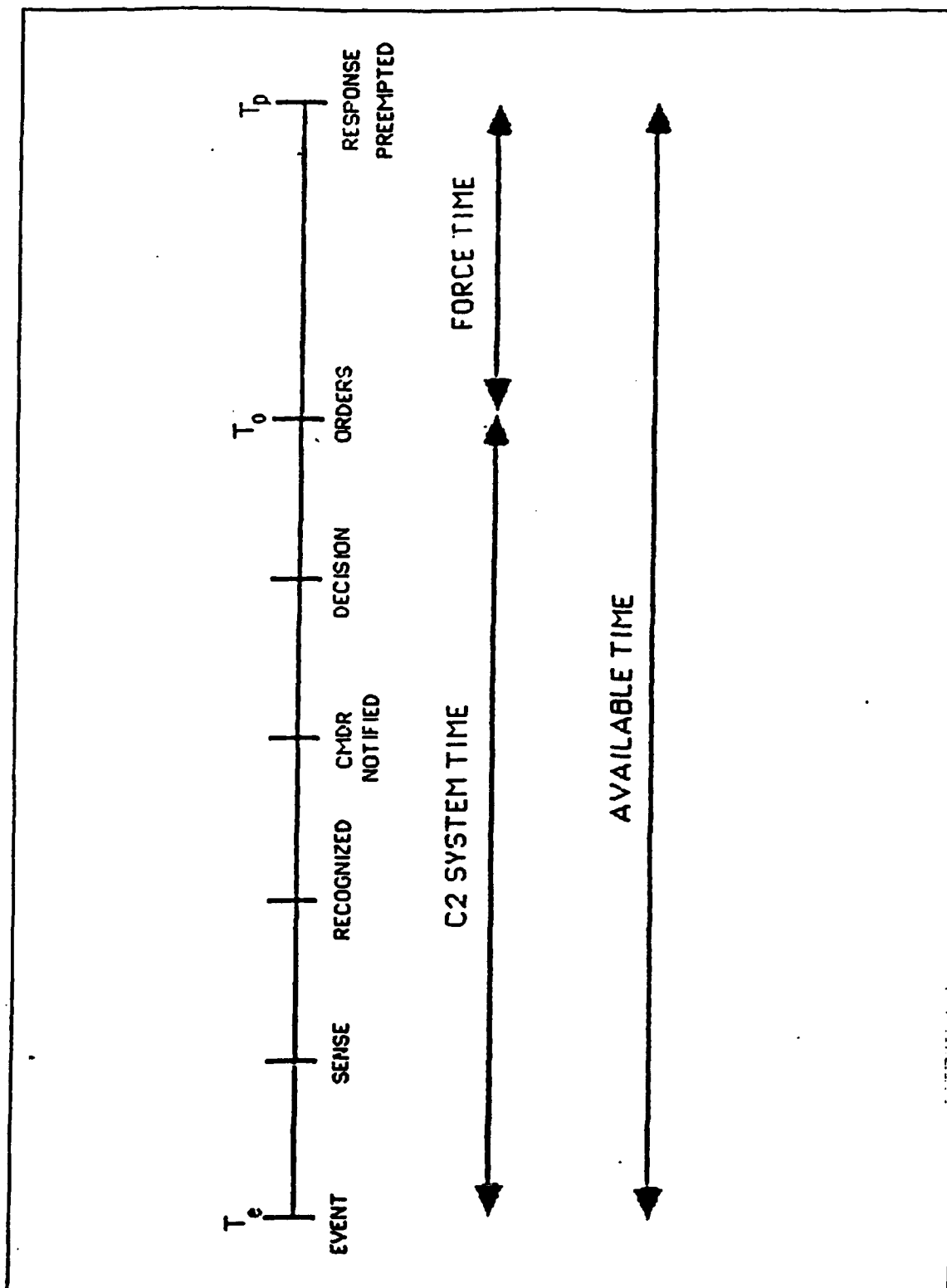
The Command and Control Differential. The C<sup>2</sup> process is a dynamic and continuous process that is based on the environment. The goal of the commander is to understand the situation and direct forces through the system faster and more effectively than the opponent. In this way the initiative and element of surprise is gained and the likelihood of success for the operations is increased.

Time is essential in the area of operations. The commander who can deploy forces at the right place and at the right time can usually do well in a crisis. To do this the commander has to find out what is going on, compare and decide what to do about it, act on the decision by directing his forces, and keep track of how the operation is going. He must perform this cycle in such a way as to force the enemy to respond defensively rather than independently planning his own actions.

The time it takes the C<sup>2</sup> process to operate plays heavily in a commander's ability to deploy forces. Figure 3 shows the dynamics of the C<sup>2</sup> process. An event requiring a response occurs at time,  $T_e$ , and the response must be completed by some later time,  $T_p$ , after which planned actions may be preempted by other events. Figure 3 shows that two major time factors make up that total time to act. These are the C<sup>2</sup> system response time,  $T_o$ , and the time



FIGURE 3  
THE COMMAND AND CONTROL DIFFERENTIAL



required by forces to act once directed,  $T_p - T_o$ .<sup>7</sup> Within the context of available time, the faster the C<sup>2</sup> process operates, the more time the forces have to act. The command and control differential between friendly and enemy forces is created by decreasing the friendly C<sup>2</sup> control cycle time or increasing the enemy's. Because of the interrelationship between the C<sup>2</sup> process, C<sup>3</sup> and the intelligence cycle, the faster and more effectively each act and interact the greater the chances are for creating the command and control differential. The efficiencies of these systems are key to the joint forces mission success.

The JFC can use a war fighting strategy to slow down the enemy C<sup>2</sup> process (or increase the cycle time) while protecting his own C<sup>2</sup> process. This strategy, C<sup>2</sup>CM is explained in the following chapter.

## CHAPTER III

### THE WAR FIGHTING STRATEGY

Throughout history commanders have realized the importance of both intelligence and deception for success in battle. Sun Tzu theorized that in battle knowledge of both your own situation and the enemy's was one of the keys to success. He recommended the use of secret agents, traps, and maneuvers to both confuse the enemy and gain information. This knowledge should then be used to both deceive the enemy and allow strikes against his most vulnerable points or, in more modern terms, centers of gravity. Sun Tzu summarized that by masking the strength of one's own military forces, the enemy could be lulled into complacency and surprised by an attack in unexpected places and at unexpected times.<sup>1</sup>

In this era of reducing military capabilities Sun Tzu's principles require greater scrutiny and integrated implementation. Concepts and strategies must be integrated at planning and execution that use a C<sup>2</sup>CM war fighting strategy to destroy or disrupt enemy C<sup>2</sup> while conserving our own process and systems. Sun Tzu's principles of "smart fighting" through deceiving and manipulating an opponent while continually striking at critical enemy command and control elements must be fully implemented as a war fighting strategy of the future. The JFC needs to use C<sup>2</sup>CM to create the C<sup>2</sup> differential. Joint Forces need to use an integrated strategy that coordinates available lethal and nonlethal means of

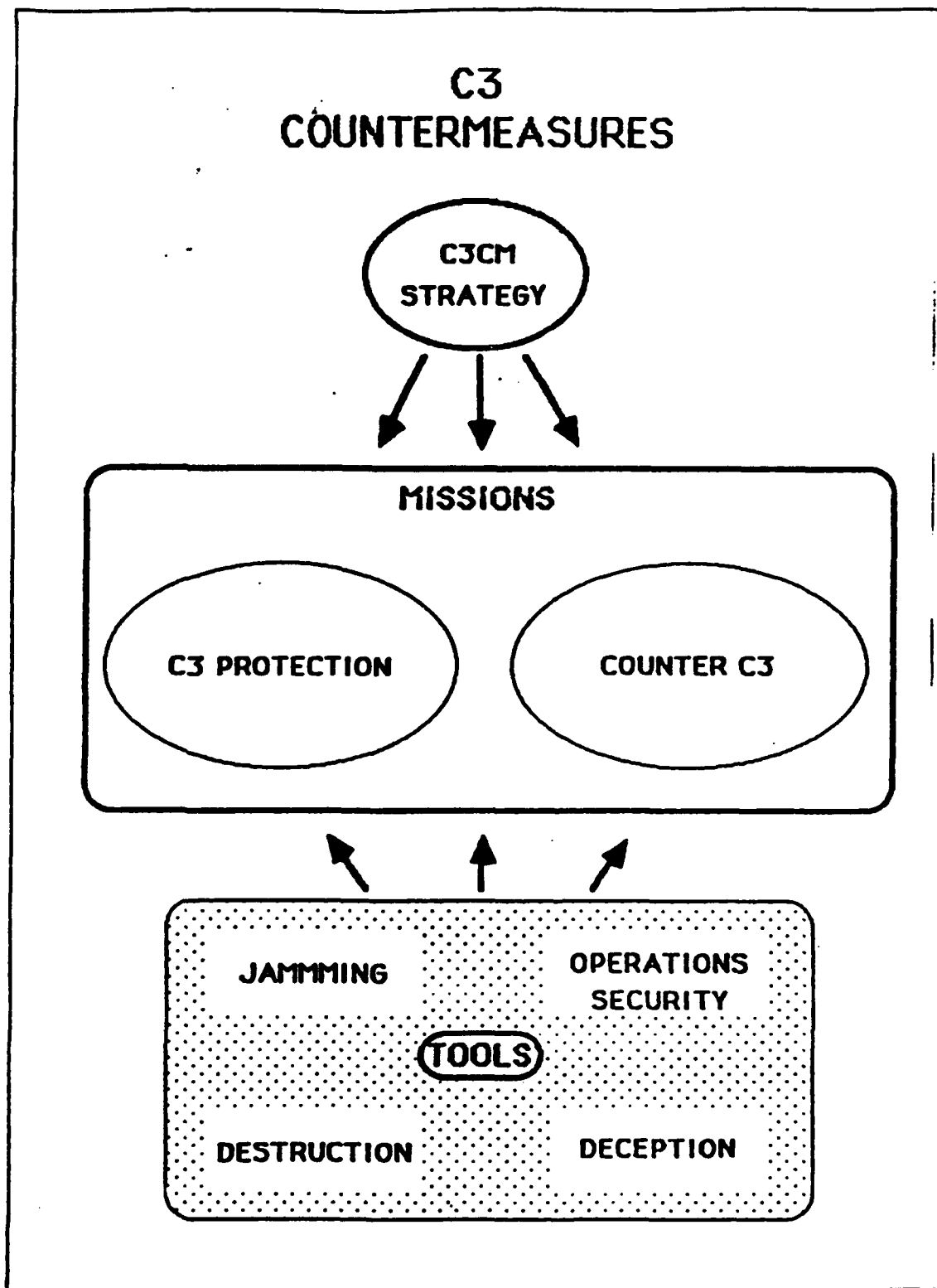
attacking an enemy's C<sup>3</sup> while protecting friendly C<sup>3</sup> capabilities.

C<sup>3</sup>CM is defined as the integrated use of operations security, military deception, jamming and physical destruction, supported by intelligence, to deny information to, influence, degrade, or destroy adversary C<sup>3</sup> capabilities and to protect friendly C<sup>3</sup> against such actions.<sup>2</sup>

The C<sup>3</sup>CM model in Figure 4 shows the relationships inherent in the C<sup>3</sup>CM definitions. The tools of the trade, OPSEC, jamming, deception, and destruction are used to perform the two noted missions to implement the total C<sup>3</sup>CM strategy.<sup>3</sup> The use of C<sup>3</sup>CM tools can best be understood by examining how they are used to support Counter C<sup>3</sup> or C<sup>3</sup> Protection activities.

Counter C<sup>3</sup>. OPSEC is the means by which weapons tactics and technology are protected from disclosure to unfriendly sources. Secure communications, TEMPEST protection, physical security, and counterintelligence all can leave the enemy guessing as to the friendly force's real intentions. OPSEC is often considered defensive in nature, but when used effectively, it can cut off the enemy's ability to anticipate friendly forces' actions. Practicing good OPSEC often can keep the enemy's intelligence gathering apparatus idle and deter the SENSE function in the enemy's C<sup>3</sup> process or it can steer the enemy's SENSE function to only receive information deliberately made available to him. By keeping our military's actions and intentions hidden, the enemy will be forced to operate in the dark. Without knowledge, the opponent will make operational decisions based on incomplete or possibly erroneous

FIGURE 4  
C<sup>3</sup>CM STRATEGY



information, thereby degrading his overall mission effectiveness.

The JFC should realize that by overdoing OPSEC the positive benefits of this tool may be overshadowed by hidden costs. The danger of "too much" OPSEC is that by concealing all friendly activities, the flow of vital information to friendly units is decreased and overall friendly control over subordinate units may be lost.

Sun Tzu realized that deception could provide commanders with the means to use surprise to strike rapidly at enemy critical nodes." Deception is a means of manipulating the enemy to act in a manner that is more beneficial to friendly forces. For deception to be accomplished, intelligence is needed on how the enemy thinks and operates, how his C<sup>2</sup> system works, what his intelligence assets are, and how he perceives friendly forces. Deception acts on the enemy's C<sup>2</sup> process by allowing his SENSE function to gather false information that is intentionally made available. Erroneous information on unit size and location, assets and capabilities, and intentions can be leaked to the enemy so that a distorted view of friendly military forces and intention is obtained. This may cause enemy decision making to be flawed so that decisions made may actually hurt their subordinate forces rather than help them. The JFC must integrate the use of deception with OPSEC and jamming for if the enemy doesn't sense the deception information deception efforts effects are reduced.

Jamming to used to degrade enemy C<sup>2</sup>. It can interrupt the communications that are needed for the C<sup>2</sup> process to operate: making it difficult for the PROCESS, COMPARE, DECIDE, and ACT

functions to perform. By disrupting sensor input or communications within a C<sup>2</sup> system, the flow of information to the commander and the rate at which he can disseminate orders is decreased.

Subsequently, his C<sup>2</sup> process is slowed. Jamming, however, is only temporary, and operators, once they realize they are being jammed, will often implement techniques that will minimize the effects.

A jamming operation should support the JFCs overall operational plan. Fragmented jamming may hinder the enemy in some aspects, but, at the same time, alert him to friendly actions. A jamming plan for the appropriate targets should be developed and executed in a concerted manner to ensure friendly actions are not intentionally given away to a perceptive enemy commander. For instance, jamming short range acquisition radars, while leaving long range early warning radars alone, will allow the enemy to prepare his defenses along the line of approach, since he will sense incoming aircraft before they get into his primary defense zone. By jamming early warning radars, the enemy reaction time and subsequent ability to get weapons on target is reduced.

Destruction is considered to be the most permanent Counter C<sup>2</sup> measure and can adversely effect any or all of the C<sup>2</sup> functions. Destruction techniques in support of Counter C<sup>2</sup> measures involve the selected use of debilitating actions to destroy identified critical parts of a C<sup>2</sup> system that implement the C<sup>2</sup> process. This surgical dissection of the C<sup>2</sup> system may be more effective than the less efficient mass destruction of units and equipment. Destruction involves the identification of critical components whose absence will cause the greatest impediment to enemy C<sup>2</sup>.

Before using destruction, questions about the effects, scope, and the length of the effects must be answered. While it may be possible to destroy some targets, it is virtually impossible to destroy every potential C<sup>2</sup> target. Destructive techniques can also be used to cause apprehension. For example, if radar sites are a primary target, radar operators, after seeing adjacent units radar assets destroyed, may hesitate to turn on their own radars. Operator apprehension may cause limited or total disruption of the remaining radar with a reduction in sensory input to the enemy C<sup>2</sup> system.

Counter C<sup>2</sup> is concerned with the effective degradation of an enemy's C<sup>2</sup> capability rather than total destruction. As mentioned, the JFC does not have the assets to destroy all C<sup>2</sup> nodes of interest. However, by applying C<sup>2</sup>CM strategy the enemy is forced to operate differently causing his operations to be degraded. Forcing the enemy to use nodes and means of communications that he does not normally use or overloading nets with traffic normally received on other networks will, almost certainly, reduce his ability to move information through the C<sup>2</sup> system and create the C<sup>2</sup> differential.

C<sup>2</sup> Protection. C<sup>2</sup> Protection consist of those activities friendly forces take to maintain the effectiveness of joint forces C<sup>2</sup> despite the enemy's and friendly counter C<sup>2</sup> actions. Understanding that everything done against an enemy can be reciprocated, the critical role of C<sup>2</sup> protection becomes evident. OPSEC is one of the key areas that the JFC can use to protect friendly capability and intentions. OPSEC is accomplished by



identifying, controlling, and protecting indicators with provide the enemy information on plans and operations.<sup>2</sup> Intelligence gathering against enemy OPSEC can be increase to keep up to date information on enemy actions to better protect against them. The ability to mask deployment, and deceive the enemy could create the C<sup>2</sup> differential and influence the outcome of the operations but the commander must be aware that even the slightest indicators may tip the enemy to friendly plans.

Protection against destruction consists of physically hardening, dispersing, or moving friendly C<sup>2</sup> sites. To protect against the enemy's capability to create the C<sup>2</sup> differential friendly forces need to protect critical C<sup>2</sup> nodes through use of hardened, redundant, mobile survivable communications assets. For protection against jamming action electronic counter-countermeasures can be used to ensure friendly effective use of the spectrum despite the enemies efforts to deny friendly use.

Counter C<sup>2</sup> requires discipline in all areas of military operations and encompasses physical, communications, electronic, emissions, transmissions and cryptographic security measures.

Intelligence and C<sup>2</sup>CM. The requirements for intelligence can be defined by the type of C<sup>2</sup>CM strategy that the JFC implements. As the commander decides how and when to use his war fighting strategy, intelligence must be tailored to support the strategy implementation. For intelligence to contribute to the war fighting strategy it must be accurate and timely. Intelligence information

must be gathered on enemy systems, capabilities and intentions for Counter C<sup>2</sup> missions. Counter C<sup>2</sup> depends on the ability to determine which adversary C<sup>2</sup> systems are the most critical for the joint actions planned or underway.<sup>6</sup> It is important to identify how the enemy is protecting his C<sup>2</sup> systems and the critical nodes. C<sup>2</sup>CM strategies require identification of the enemy's EEI needs and his means of intelligence collection and processing. Friendly intelligence needs to provide information to the JFC for direction and redirection of C<sup>2</sup>CM efforts with timely feedback to determine effectiveness. The JFC needs intelligence for his C<sup>2</sup>CM strategy that is:

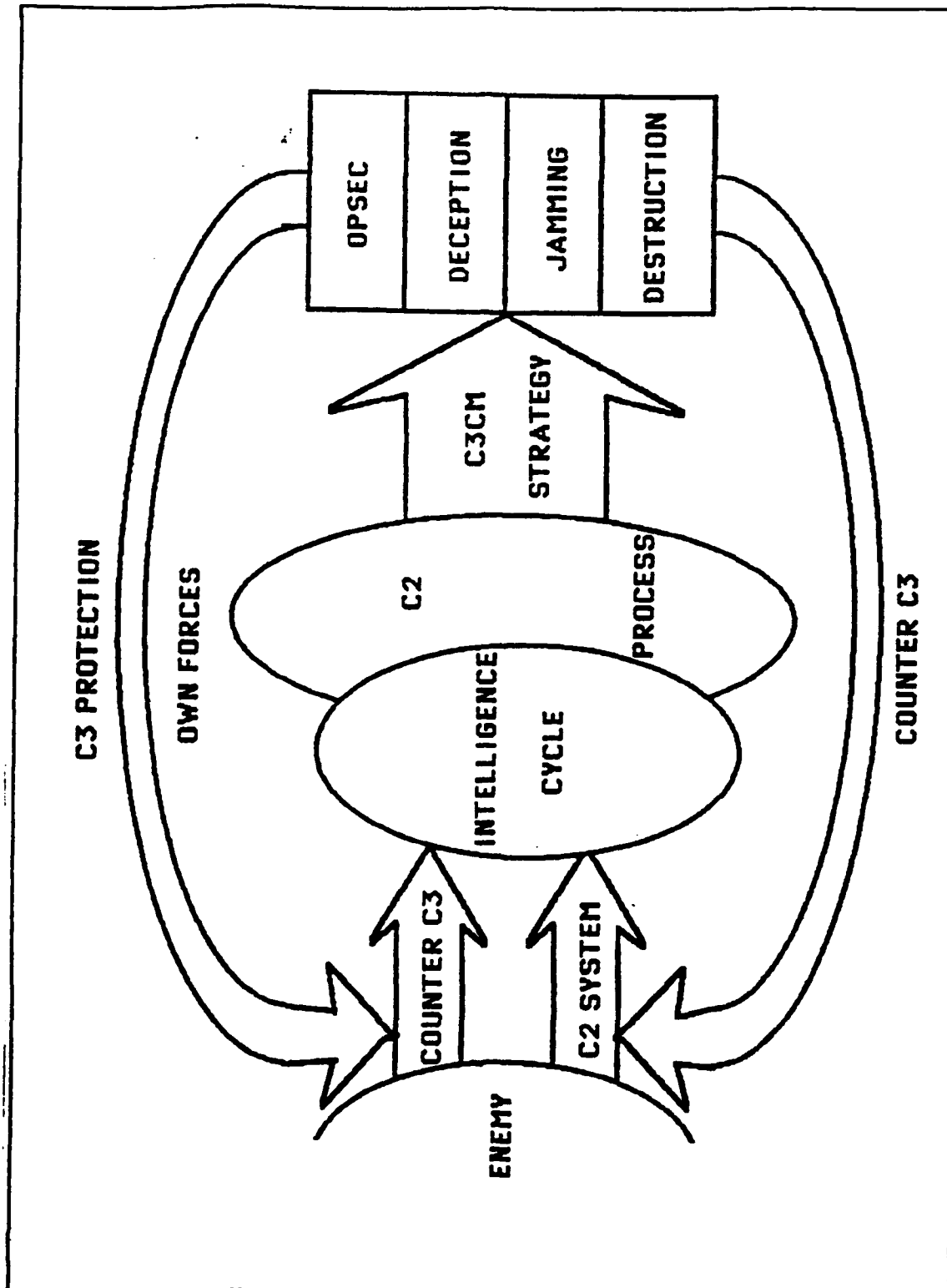
- \* obtained from all sources of collection
- \* Real time or as near as possible
- \* over an extended geography and a deep look
- \* based on systems that are interoperable and are able to function in a joint environment.

Intelligence on enemy C<sup>2</sup> is necessary to properly plan C<sup>2</sup>CM. It is clear without intelligence C<sup>2</sup>CM tools are ineffective and Counter C<sup>2</sup> and C<sup>2</sup> Protection can not be accomplished.

There is a direct interrelationship between the intelligence cycle, C<sup>2</sup> and C<sup>2</sup>CM. Figure 5 show how intelligence impacts on the C<sup>2</sup> process and C<sup>2</sup>CM strategy. C<sup>2</sup>CM is implemented through the C<sup>2</sup> process. Decisions that commanders make are guided by the tailored intelligence produced in the intelligence cycle. This cycle produces intelligence both on the enemy's C<sup>2</sup> systems and the protection to his C<sup>2</sup> systems. The commander then makes a decision to employ the tools of C<sup>2</sup>CM to attack the enemy's attempts to

FIGURE 5

C<sup>3</sup>CM, INTELLIGENCE AND C<sup>2</sup> PROCESS



protect his C<sup>2</sup> or disrupts the enemy C<sup>2</sup> systems.

Conclusions. Counter C<sup>2</sup> and C<sup>2</sup> Protection activities do more than just counter or protect C<sup>2</sup>. These C<sup>2</sup>CM strategies should be used in conjunction with other strategies of war in order to bring the best combination of lethal and nonlethal assets to bear on the enemy at the right place and the right time. C<sup>2</sup>CM can create the C<sup>2</sup> differential by preventing the enemy from effectively using his C<sup>2</sup> system to counter other offensive actions.

The key problems facing the JFC in implementing C<sup>2</sup>CM are integrating and blending the options, techniques and capabilities inherent in the component commands. Desert Storm proved that electronics are pervasive throughout the joint command, not just in communications, intelligence and electronic warfare systems.<sup>7</sup> Integrating C<sup>2</sup>CM throughout the command requires the JFC have experts working together as a team to take advantage of the benefits of this war fighting strategy. The next chapter offers suggestions for improving the planning and implementation of joint C<sup>2</sup>CM.

## CHAPTER IV

### IMPLEMENTING C<sup>3</sup>CM

'Effectively integrated joint forces expose no weak point or seams to enemy actions, while they rapidly and efficiently find and attack enemy weak points.'"<sup>1</sup> This chapter offers suggestions for the JFC to accomplish the above goal while implementing C<sup>3</sup>CM.

C<sup>3</sup>CM in the Joint Environment: Integrated, Synchronized, Coordinated. C<sup>3</sup>CM principles must be integrated into a war fighting strategy at the joint level. Integrated employment of C<sup>3</sup>CM is the essence of the war fighting strategy.<sup>2</sup> It is necessary to have a coordinated plan from the JFC to achieve superior C<sup>3</sup> and synchronize actions against adversary C<sup>3</sup>. Too often C<sup>3</sup>CM is included as an afterthought without realizing its potential to seize the initiative during an operation. It is through the joint, synchronized planning and execution of deception, OPSEC, jamming and destruction that the C<sup>3</sup> differential can be attained. C<sup>3</sup>CM must be part of operations planning.

The Navy has developed a plan to establish a separate electronic warfare and space commander reporting to the Navy Component Commander. The purpose is to integrate communications, intelligence and electronic warfare assets and techniques with one commander to provide a synchronized war fighting strategy.<sup>3</sup> The lesson for the JFC is that this type of warfare requires dedicated

commanders and staff to be successful in joint operations. First, the JFC should have a team of dedicated experts in operations, intelligence, communications, and component commands C<sup>3</sup>CM capabilities to plan and execute C<sup>3</sup>CM as an integrated, synchronized and coordinated war fighting strategy. Through the use of a team of experts the JFC can know what his C<sup>3</sup>, intelligence and C<sup>3</sup>CM assets are, plan for an integrated C<sup>3</sup>CM strategy, and use service C<sup>3</sup>CM assets that are mutually supportive to the overall operations. Secondly, in the future the JFC may find it necessary to appoint a joint force component commander responsible for C<sup>3</sup>CM, space and electronic warfare similar to the Navy's concept to control and deconflict the myriad of employment options.

Guarding the Indicators. Counter C<sup>3</sup> measures are the most difficult to implement and measure the effectiveness. Often in times of crisis protecting friendly C<sup>3</sup> efforts suffer either through neglect, time factors or ignorance. OPSEC requires constant vigilance and forethought. The JFC must establish clear cut direction prior to hostilities and enforce those directives. The JFC and staff must control tertiary variations in actions that give the adversary clues to friendly actions. Prior to the commencement of the Desert Storm air raid over Baghdad, Iraqis could have estimated the time of attack by monitoring the phone lines of pizza shops in northern Virginia. There was a noticeable increase in rush pizza delivery orders from staffers who were working late at the Pentagon.<sup>4</sup>

The JFC and staff must regulate changes in communications

patterns that provide information on actions. At the Headquarters, European Command, during a classified operation in one of the African countries, unclassified telephone operators knew that a crisis was occurring and knew the country it was occurring in from the pattern and frequency of calls they were asked to place.

The JFC and staff must institute and practice habits in day to day operations that will provide operations security during war. For instance at the beginning Desert Shield, critical C<sup>2</sup> circuit outages were not classified. Adversaries could have gleaned essential information about the most critical C<sup>2</sup> nodes by monitoring signalers conversations about C<sup>2</sup> outages. After several days, this information became classified. Difficulties resulted because this required instituting practices that had not been exercised previously. What should have been second nature and a matter of habit was not because OPSEC in this area had not been instituted in day to day operations.

Fixing Joint Intelligence Cycle and C<sup>2</sup> Capabilities. C<sup>2</sup>CM efforts are inextricably linked to the efficiency of friendly intelligence efforts and communications capabilities. C<sup>2</sup> systems provide the JFC with critical and relevant information, in time to make the difficult war fighting decisions. C<sup>2</sup> systems provide the medium for the command and control process to function. The more relevant, timely and concise the medium the more efficiently the C<sup>2</sup> process will function. Key to the effectiveness of the C<sup>2</sup> process is a correlated intelligence cycle that is responsive to requests

for essential elements of information.

Lessons from Desert Storm indicate that there are illnesses in intelligence and communications capabilities that must be cured. Joint interoperability is not a principle that can be assumed by the JFC. A review of the Desert Storm lessons learned showed problems such as: intelligence systems not designed to withstand the rigors of combat; different C<sup>2</sup> procedures for the U.S. Marine Corps support to maritime and land operations; inability to communicate with coalition forces; lack of centralized control of communications; and overloaded communications systems preventing units from obtaining needed intelligence. In addition, there were no operational C<sup>2</sup> plans during the first four months of the Desert Shield and no frequency management for several weeks. Problems with secondary dissemination of intelligence data in theater caused users difficulties with intelligence timeliness, accuracy and usefulness."

Intelligence and communications assets must function properly to ensure that C<sup>2</sup>CM is implemented and the feedback required to ensure the effectiveness of joint C<sup>2</sup>CM strategy is provided. If the intelligence and communication problems are not repaired we can create a negative C<sup>2</sup> differential that benefits the adversary while degrading our own C<sup>2</sup> process. In future operations, commanders must ensure that we are not our own worst enemy and cure the intelligence and communications problems.



## CHAPTER V

### CONCLUSION

For success in the high technology wars of the future the JFC must plan, practice and execute integrated and synchronized joint C<sup>3</sup>CM to create the C<sup>2</sup> differential. The joint and coordinated use of C<sup>3</sup>CM assets generates an opportunity not only to compensate for the weak areas in the component commands assets but also to obtain an intensifying effect. Land, sea, air, special operations and space assets all contribute to the joint commanders ability to defeat the C<sup>2</sup> capabilities of the enemy.

C<sup>3</sup>CM is an effective war fighting strategy that is aimed at the enemy's C<sup>2</sup> process, communications and intelligence cycles while protecting friendly capabilities to control forces. For the joint strategy to be most effective it needs to be planned and directed by a team of experts on the joint staff. Joint Commanders need to emphasize C<sup>2</sup> Protection missions with a concentration on CPSEC. Continued emphasis needs to be placed on making our communications and intelligence capabilities interoperable and effective among the component commands for continued joint success.

In the future, strategic objectives may be met by linking joint assets in a C<sup>3</sup>CM strategy to debilitate the enemy's ability to control his forces in conflict. When the C<sup>2</sup> differential is gained and the enemy commander can no longer control his forces his defeat is virtually assured. Joint C<sup>3</sup>CM strategy can be most effective because its aim is to defeat the commander. JFC can render enemy

commanders helpless by employing joint C3CM strategies. B.H. Lidell Hart states that "It is in the minds of the commander that the issue of battle is really decided".<sup>1</sup> The JFC can use C<sup>3</sup>CM to attack the minds of the enemy commanders and meet our strategic military objectives while conserving our forces.

## NOTES

### Chapter I

1. Ralph W. Shrader, "C4I: Desert Storm's Unsung Technology Superstar," Signal, May 1991, p. 15
2. John H. Wickham, "Desert Storm Stirs Up Debate On Weapons Need," Signal, August 1991, p. 15
3. U.S. Department of Defense, Joint Warfare of the US Armed Forces, Joint Publication 1, (Washington D.C.: 1991) pp. 22-23
4. U.S. Department of Defense, A Doctrinal Statement of Selected Joint Operational Concepts, (Washington, D.C.:1992) p.6
5. U.S. Department of Defense, Joint Warfare of the US Armed Forces, Joint Publication 1, (Washington D.C.: 1991) pp. 38-39

### Chapter II

1. Defense Systems, Inc., Elements of C<sup>2</sup> Theory, DCA 100-84-C-0047 (Washington, D.C., 1985) p. 77
2. Department of Defense, Doctrine For Command, Control, Communications and Computers (C4) Systems Support to Joint Operations, Joint Publication 6-0 (Washington:1992) p. 11-1

3. Joel S. Lawson, "The State Variables of a Command Control System," Proceedings for Quantitative Assessment of the Utility of Command and Control Systems, (Washington, D.C. 1980) pp. 93-99

4. George E. Orr, Combat Operations C<sup>3</sup>I: Fundamentals and Interactions, (Air War College, AI: 1983) pp. 28-29

5. U.S. Department of Defense, Department of Defense Directive 4600.4 (Washington D.C.: 1979) p. 1

6. U.S. Department of Defense, Joint Chiefs of Staff Publication 1, (Washington D.C.: 1979) p. 177

7. Elements of C<sup>3</sup> Theory, p. 85

### Chapter III

1. Sun Tzu, The Art of War, translated by Samuel B. Griffith (London: Oxford Press, 1963) pp. 66-84

2. U.S. Department of Defense, Command, Control, and Communications Countermeasures in Joint Military Operations, Joint Publication 28, (Washington D.C.: 1987) p x

3. Joint Publication 28, p. xi

4. Sun Tzu, p. 38

5. Joint Publication 28, p. xii

6. Joint Publication 28, p. iv-4

7. Clarence A. Robinson, "Electronic Battlefield's Exposure Bolsters Army", Signal, August 1991, p 19

#### Chapter IV

1. U.S. Department of Defense, A Doctrinal Statement of Selected Joint Operational Concepts, (Washington, D.C.:1992) p.1

2. Department of Defense, Command, Control, and Communications Countermeasures in Joint Military Operations, Joint Publication 28, (Washington D.C.: 1987) p II-2

3. From briefing on Navy Space Command, Lecture, U.S. Naval War College, Newport R.I., 17 Feb 92

4. James F. Dunnigam and Austin Bay, From Shield to Storm, (New York:1992) p.143

5. Joint Universal Lessons Learned. "Desert Storm/Command and Control/Intelligence." JULLS Database, 1993

## Chapter V

1. B.H. Liddell Hart, quoted in Robert Debs Heinl, Dictionary of Military and Naval Quotations, (Maryland:1966) p. 61

## BIBLIOGRAPHY

Bay, Austin and Dunnigam, James F. From Shield to Storm. New York: William Morrow and Company Inc. 1992

Defense Systems, Inc. Elements of C<sup>2</sup> Theory. DCA 100-84-C-0047  
Washington, D.C.: 1985

Heinl, Robert Debs, Dictionary of Military and Naval Quotations,  
Maryland: United States Naval Institute. 1966

Joint Universal Lessons Learned. "Desert Storm/Command and  
Control/Intelligence." JULLS Database, 1993

Lawson, Joel S. "The State Variables of a Command Control System."  
Proceedings for Quantitative Assessment of the Utility of  
Command and Control Systems. Washington, D.C.: 1980

Navy Space Command Briefing, Lecture, U.S. Naval War College,  
Newport R.I: 17 Feb 92

Orr, George E. Combat Operations C<sup>2</sup>I: Fundamentals and  
Interactions. Air War College, AI: 1983

Robinson, Clarence A. "Electronic Battlefield's Exposure Bolsters  
Army". Signal. August 1991 pp. 19-25

Shrader, Ralph W. "C4I: Desert Storm's Unsung Technology  
Superstar." Signal, May 1991, p. 15

Sun Tzu, The Art of War, translated by Samuel B. Griffith. London:  
Oxford Press, 1963

U.S. Department of Defense. A Doctrinal Statement of Selected Joint  
Operational Concepts. Washington, D.C.:1992

U.S. Department of Defense. Command, Control, and Communications  
Countermeasures in Joint Military Operations. Joint Publication  
28, Washington D.C.: 1987

U.S. Department of Defense. Department of Defense Directive 4600.4  
Washington D.C.: 1979

U.S. Department of Defense. Doctrine For Command, Control,  
Communications and Computers (C4) Systems Support to Joint  
Operations. Joint Publication 6-0. Washington:1992

U.S. Department of Defense. Joint Chiefs of Staff Publication 1.  
Washington D.C.: 1979

U.S. Department of Defense. Joint Warfare of the US Armed Forces.  
Joint Publication 1. Washington D.C.: 1991.



Nickham, John H. "Desert Storm Stirs Up Debate On Weapons Need."

Signal, August 1991, p. 15